

# RSA 密码破译报告

冯古豪

PKU EECS

2022 年 6 月 4 日

## 1 RSA 加密原理

## 2 攻击方式和实验结果

- 基于低加密指数的攻击
- 维纳攻击
- 基于大数分解的攻击
- 其他攻击方式

# 欧拉定理

## 定理

$a, n$  为两个互素的正整数, 则  $a^{\phi(n)} \equiv 1 \pmod{n}$ , 其中  $\phi(n)$  为欧拉函数。

# RSA 加密

RSA 加密算法首先生成出两个大素数  $p, q$ ，要加密的二进制数记为  $m$ ，公共模数  $n = pq$ ，公钥  $e$  为任意一个小于  $\phi(n)$  的正整数。私钥  $d$  满足  $e \times d \equiv 1 \pmod{\phi(n)}$ ，加密后我们发送的数字  $c = m^e \pmod{n}$ 。在解密时，有  $m = c^d \pmod{n}$ ，其中，公钥为  $c$  公开的，私钥  $d$  只有通信两方掌握。

# 低加密指数攻击

算法原理

实验结果

# 低加密指数广播攻击

算法原理

实验结果

# Corper-Smith 攻击

算法原理

实验结果

# 维纳攻击

算法原理

实验结果



# 费马分解

算法原理

实验结果

# Pollard- $p-1$ 分解

算法原理

实验结果

# Pollard- $\rho$ 分解

算法原理

实验结果

# 公因数分解

算法原理

实验结果

# 共模攻击

算法原理

实验结果

# 谢谢大家